

Cisco

Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking



NEW QUESTION 1

You want to store files that will be accessible by every user on your network. Which endpoint device do you need?

- A. Access point
- B. Server
- C. Hub
- D. Switch

Answer: B

Explanation:

To store files that will be accessible by every user on a network, you would need a server. A server is a computer system that provides data to other computers. It can serve data to systems on a local network (LAN) or a wide network (WAN) over the internet. In this context, a file server would be set up to store and manage files, allowing users on the network to access them from their own devices1.

References :=

? What is a Server?

? Understanding Servers and Their Functions

A server is a computer designed to process requests and deliver data to other computers over a local network or the internet. In this case, to store files that will be accessible by every user on the network, a file server is the appropriate endpoint device. It provides a centralized location for storing and managing files, allowing users to access and share files easily.

? A. Access point: Provides wireless connectivity to a network.

? C. Hub: A basic networking device that connects multiple Ethernet devices together, making them act as a single network segment.

? D. Switch: A networking device that connects devices on a computer network by using packet switching to forward data to the destination device.

Thus, the correct answer is B. Server.

References :=

? File Server Overview (Cisco)

? Server Roles in Networking (Cisco)

NEW QUESTION 2

A user initiates a trouble ticket stating that an external web page is not loading. You determine that other resources both internal and external are still reachable. Which command can you use to help locate where the issue is in the network path to the external web page?

- A. ping -t
- B. tracert
- C. ipconfig/all
- D. nslookup

Answer: B

Explanation:

The tracert command is used to determine the route taken by packets across an IP network. When a user reports that an external web page is not loading, while other resources are accessible, it suggests there might be an issue at a certain point in the network path to the specific web page. The tracert command helps to diagnose where the breakdown occurs by displaying a list of routers that the packets pass through on their way to the destination. It can identify the network segment where the packets stop progressing, which is valuable for pinpointing where the connectivity issue lies. References := Cisco CCST Networking Certification FAQs – CISCONET Training Solutions, Command Prompt (CMD): 10 network-related commands you should know, Network Troubleshooting Commands Guide: Windows, Mac & Linux - Comparitech, How to Use the Traceroute and Ping Commands to Troubleshoot Network, Network Troubleshooting Techniques: Ping, Traceroute, PathPing.

•tracert Command: This command is used to determine the path packets take to reach a destination. It lists all the hops (routers) along the way and can help identify where the delay or failure occurs.

•ping -t: This command sends continuous ping requests and is useful for determining if a host is reachable but does not provide path information.

•ipconfig /all: This command displays all current TCP/IP network configuration values and can be used to verify network settings but not to trace a network path.

•nslookup: This command queries the DNS to obtain domain name or IP address mapping, useful for DNS issues but not for tracing network paths. References:

•Microsoft tracert Command: tracert Command Guide

•Troubleshooting Network Issues with tracert: Network Troubleshooting Guide

NEW QUESTION 3

DRAG DROP

Move each protocol from the list on the left to its correct example on the right.

Move each protocol from the list on the left to its correct example on the right.

Protocols

DHCP

DNS

ICMP

Examples

Perform a query to translate companypro.net to an IP address.

Assign the reserved IP address 10.10.10.200 to a web server at your company.

Perform a ping to ensure that a server is responding to network connections.

Protocol

Protocol

Protocol

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The correct matching of the protocols to their examples is as follows:

? DHCP: Assign the reserved IP address 10.10.10.200 to a web server at your company.

? DNS: Perform a query to translate companypro.net to an IP address.

? ICMP: Perform a ping to ensure that a server is responding to network connections.

Here's how each protocol corresponds to its example:

? DHCP (Dynamic Host Configuration Protocol) is used to assign IP addresses to devices on a network. In this case, DHCP would be used to assign the reserved IP address 10.10.10.200 to a web server.

? DNS (Domain Name System) is used to translate domain names into IP addresses. Therefore, to translate companypro.net to an IP address, DNS would be utilized.

? ICMP (Internet Control Message Protocol) is used for sending error messages and operational information indicating success or failure when communicating with another IP address. An example of this is using the ping command to check if a server is responding to network connections.

These protocols are essential for the smooth operation of networks and the internet.

? Perform a query to translate companypro.net to an IP address.

? Assign the reserved IP address 10.10.10.200 to a web server at your company.

? Perform a ping to ensure that a server is responding to network connections.

? DNS (Domain Name System): DNS translates human-friendly domain names like "companypro.net" into IP addresses that computers use to identify each other on the network.

? DHCP (Dynamic Host Configuration Protocol): DHCP automatically assigns IP addresses to devices on a network, ensuring that no two devices have the same IP address.

? ICMP (Internet Control Message Protocol): ICMP is used for diagnostic or control purposes, and the ping command uses ICMP to test the reachability of a host on an IP network.

References:

? DNS Basics: What is DNS?

? DHCP Overview: What is DHCP?

? ICMP and Ping: Understanding ICMP

NEW QUESTION 4

Which address is included in the 192.168.200.0/24 network?

- A. 192.168.199.13
- B. 192.168.200.13
- C. 192.168.201.13
- D. 192.168.1.13

Answer: B

Explanation:

•192.168.200.0/24 Network: This subnet includes all addresses from 192.168.200.0 to 192.168.200.255. The /24 indicates a subnet mask of 255.255.255.0, which allows for 256 addresses.

•192.168.199.13: This address is in the 192.168.199.0/24 subnet, not the 192.168.200.0/24 subnet.

•192.168.200.13: This address is within the 192.168.200.0/24 subnet.

•192.168.201.13: This address is in the 192.168.201.0/24 subnet, not the 192.168.200.0/24 subnet.

•192.168.1.13: This address is in the 192.168.1.0/24 subnet, not the 192.168.200.0/24 subnet.

References:

•Subnetting Guide: Subnetting Basics

NEW QUESTION 5

Which command will display all the current operational settings configured on a Cisco router?

- A. show protocols
- B. show startup-config
- C. show version
- D. show running-config

Answer: D

Explanation:



Router

The show running-config command is used on a Cisco router to display the current operational settings that are actively configured in the router's RAM. This command outputs all the configurations that are currently being executed by the router, which includes interface configurations, routing protocols, access lists, and other settings. Unlike show startup-config, which shows the saved configuration that the router will use on the next reboot, show running-config reflects the live, current configuration in use.

References := The information is supported by multiple sources that detail the use of Cisco commands, particularly the show running-config command as the standard for viewing the active configuration on a Cisco device¹²³.

? show running-config: This command displays the current configuration running on the router. It includes all the operational settings and configurations applied to the router.

? show protocols: This command shows the status of configured protocols on the router but not the entire configuration.

? show startup-config: This command displays the configuration saved in NVRAM, which is used to initialize the router on startup, but not necessarily the current running configuration.

? show version: This command provides information about the router's software version, hardware components, and uptime but does not display the running configuration.

References:

? Cisco IOS Commands: Cisco IOS Commands

NEW QUESTION 6

HOTSPOT

An app on a user's computer is having problems downloading data. The app uses the following URL to download data:

<https://www.companypro.net:7100/api>

You need to use Wireshark to capture packets sent to and received from that URL. Which Wireshark filter options would you use to filter the results? Complete the command by selecting the correct option from each drop-down list. Note: You will receive partial credit for each correct selection.

<div> <div></div> <div>tcp</div> <div>udp</div> </div>	.	<div> <div></div> <div>port</div> <div>user_agent</div> </div>	==	<div> <div></div> <div>7100</div> <div>companypro.net</div> <div>http</div> </div>
--	---	--	----	--

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To capture packets sent to and received from the URL <https://www.companypro.net:7100/api> using Wireshark, you would use the following filter options:

? Protocol: tcp

? Filter Type: port

? Port Number: 7100

This filter setup in Wireshark will display all TCP packets that are sent to or received from port 7100, which is the port specified in the URL for the API service. Since HTTPS typically uses TCP as the transport layer protocol, filtering by TCP and the specific port number will help isolate the relevant packets for troubleshooting the app's data download issues.

? cp: The app is using HTTPS, which relies on the TCP protocol for communication.

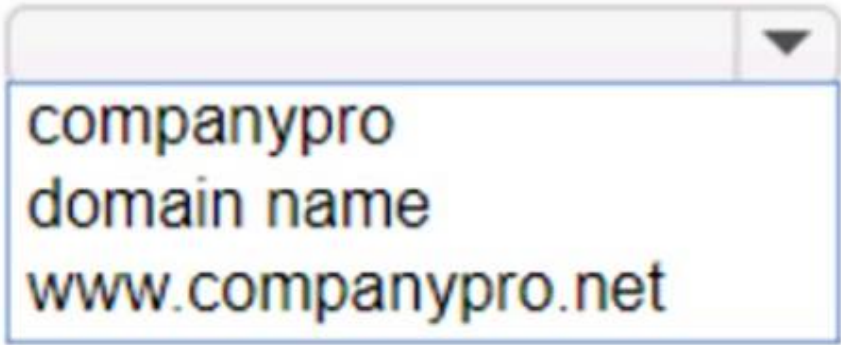
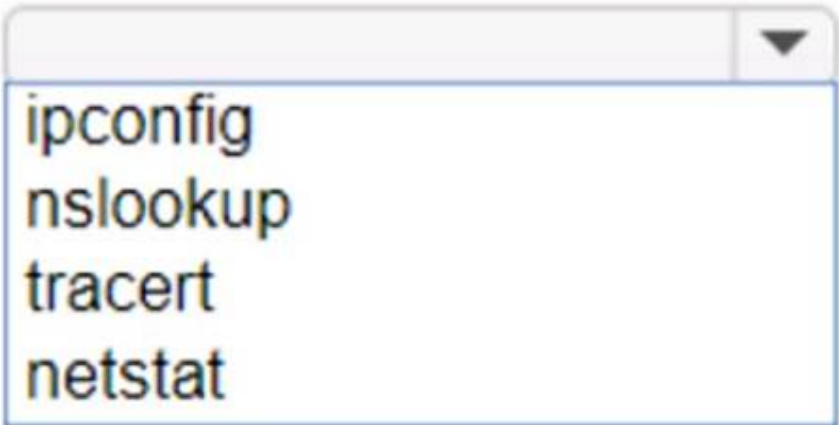
? port: The specific port number used by the application, which in this case is 7100.

? 7100: This is the port specified in the URL (<https://www.companypro.net:7100/api>). This filter will capture all TCP traffic on port 7100, allowing you to analyze the packets related to the application's data download.
References:
? Wireshark Filters: Wireshark Display Filters

NEW QUESTION 7

HOTSPOT

You want to list the IPv4 addresses associated with the host name `www.companypro.net`.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To list the IPv4 addresses associated with the host name `www.companypro.net`, you should use the following command:
`nslookup www.companypro.net`
This command will query the DNS servers to find the IP address associated with the hostname provided. If you want to ensure that it returns the IPv4 address, you can specify the `-type=A` option, which stands for Address records that hold IPv4 addresses¹. However, the `nslookup` command by default should return the IPv4 address if available.
To list the IPv4 addresses associated with the host name `www.companypro.net`, you should use the `nslookup` command.
? Command: `nslookup`
? Target: `www.companypro.net` So, the completed command is:
? `nslookup www.companypro.net`
? `nslookup`: This command is used to query the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
? `www.companypro.net`: This is the domain name you want to query to obtain its associated IP addresses. References:
? Using `nslookup`: `nslookup` Command Guide

NEW QUESTION 8

For each statement about bandwidth and throughput, select True or False.
Note: You will receive partial credit for each correct selection.

For each statement about bandwidth and throughput, select **True** or **False**.

Note: You will receive partial credit for each correct selection.

Answer Area

	True	False
Low bandwidth can increase network latency.	<input type="radio"/>	<input type="radio"/>
High levels of network latency decrease network bandwidth.	<input type="radio"/>	<input type="radio"/>
You can increase throughput by decreasing network latency.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

? Statement 1: Low bandwidth can increase network latency.
? Statement 2: High levels of network latency decrease network bandwidth.

? Statement 3: You can increase throughput by decreasing network latency.
? Bandwidth vs. Latency: Bandwidth refers to the maximum rate at which data can be transferred over a network path. Latency is the time it takes for a data packet to travel from the source to the destination.
References:
? Network Performance Metrics: Cisco Network Performance
? Understanding Bandwidth and Latency: Bandwidth vs. Latency

NEW QUESTION 9

You plan to use a network firewall to protect computers at a small office.
For each statement about firewalls, select True or False. Note: You will receive partial credit for each correct selection.

	True	False
A firewall can direct all web traffic to a specific IP address.	<input type="radio"/>	<input type="radio"/>
A firewall can block traffic to specific ports on internal computers.	<input type="radio"/>	<input type="radio"/>
A firewall can prevent specific apps from running on a computer.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

? A firewall can direct all web traffic to a specific IP address.
? A firewall can block traffic to specific ports on internal computers.
? A firewall can prevent specific apps from running on a computer.
? Directing Web Traffic: Firewalls can manage traffic redirection using NAT and port forwarding rules to route web traffic to designated servers or devices within the network.
? Blocking Specific Ports: Firewalls can enforce security policies by blocking or allowing traffic based on port numbers, ensuring that only permitted traffic reaches internal systems.
? Application Control: While firewalls manage network traffic, preventing applications from running typically requires software specifically designed for endpoint protection and application management.
References:
? Understanding Firewalls: Firewall Capabilities

NEW QUESTION 10

HOTSPOT
You purchase a new Cisco switch, turn it on, and connect to its console port. You then run the following command:

```
#show running-config | section include interface
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
<output omitted>
```

For each statement about the output, select True or False. Note: You will receive partial credit for each correct selection.

	True	False
The two interfaces are administratively shut down.	<input type="radio"/>	<input type="radio"/>
The two interfaces have default IP addresses assigned.	<input type="radio"/>	<input type="radio"/>
The two interfaces can communicate over Layer 2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- ? The two interfaces are administratively shut down:
 - ? The two interfaces have default IP addresses assigned:
 - ? The two interfaces can communicate over Layer 2:
 - ? Interface Status: The absence of the "shutdown" command means the interfaces are not administratively shut down.
 - ? IP Address Assignment: There is no evidence in the output that IP addresses have been assigned to the interfaces, which would typically be shown as "ip address" entries.
 - ? Layer 2 Communication: Switch interfaces in their default state operate at Layer 2, enabling them to forward Ethernet frames and participate in Layer 2 communication.
- References:
- ? Cisco IOS Interface Configuration: Cisco Interface Configuration
 - ? Understanding Cisco Switch Interfaces: Cisco Switch Interfaces

NEW QUESTION 10

HOTSPOT

Computers in a small office are unable to access companypro.net. You run the ipconfig command on one of the computers. The results are shown in the exhibit.
You need to determine if you can reach the router.

```
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.0.14(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, January 8, 2023 11:00:02 AM
Lease Expires . . . . . : Sunday, January 8, 2023 12:00:12 PM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled
```

Which command should you use? Complete the command by selecting the correct options from each drop-down lists.

netstat
ping
ftp
nslookup

companypro.net
192.168.0.1
localhost
8.8.8.8

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To determine if you can reach the router, you should use the ping command followed by the IP address of the router. The ping command is a network utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination

computer.

The Default Gateway in the ipconfig results is typically the router's IP address in a home or small office network. In this case, the Default Gateway is 192.168.0.1, which is the address you would ping to check connectivity to the router.

References :=

? How to Use the Ping Command

? Testing Network Connectivity with the Ping Command

=====

To determine if you can reach the router, you should use the ping command with the IP address of the router.

? Command: ping

? Target: 192.168.0.1 So, the completed command is:

? ping 192.168.0.1

Step by Step Comprehensive and Detailed Explanation:

? ping: The ping command sends ICMP Echo Request messages to the target IP address and waits for an Echo Reply. It is commonly used to test the reachability of a network device.

? 192.168.0.1: This is the IP address of the default gateway (the router) as shown in the ipconfig output. Pinging this address will help determine if the computer can communicate with the router.

References:

? Using the ping Command: ping Command Guide

NEW QUESTION 12

DRAG DROP

Move each protocol from the list on the left to the correct TCP/IP model layer on the right. Note: You will receive partial credit for each correct match.

Protocols

TCP

IP

FTP

Ethernet

TCP Model Layer

Application

Transport

Internetwork

Network

Protocol

Protocol

Protocol

Protocol

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Here's how each protocol aligns with the correct TCP/IP model layer:

? TCP (Transmission Control Protocol): This protocol belongs to the Transport layer, which is responsible for providing communication between applications on different hosts1.

? IP (Internet Protocol): IP is part of the Internetwork layer, which is tasked with routing packets across network boundaries to their destination1.

? FTP (File Transfer Protocol): FTP operates at the Application layer, which supports application and end-user processes. It is used for transferring files over the network1.

? Ethernet: While not a protocol within the TCP/IP stack, Ethernet is associated with the Network Interface layer, which corresponds to the link layer of the TCP/IP model and is responsible for the physical transmission of data1.

The TCP/IP model layers are designed to work collaboratively to transmit data from one layer to another, with each layer having specific protocols that perform functions necessary for the data transmission process1.

? TCP:

? IP:

? FTP:

? Ethernet:

? Transport Layer: This layer is responsible for providing communication services directly to the application processes running on different hosts. TCP is a core protocol in this layer.

? Internetwork Layer: This layer is responsible for logical addressing, routing, and packet forwarding. IP is the primary protocol for this layer.

? Application Layer: This layer interfaces directly with application processes and provides common network services. FTP is an example of a protocol operating in this layer.

? Network Layer: In the TCP/IP model, this layer includes both the data link and physical layers of the OSI model. Ethernet is a protocol used in this layer to define network standards and communication protocols at the data link and physical levels.

References:

? TCP/IP Model Overview: Cisco TCP/IP Model

? Understanding the TCP/IP Model: TCP/IP Layers

NEW QUESTION 13

During the data encapsulation process, which OSI layer adds a header that contains MAC addressing information and a trailer used for error checking?

- A. Network
- B. Transport
- C. Data Link
- D. Session

Answer: C

Explanation:



OSI model

During the data encapsulation process, the Data Link layer of the OSI model is responsible for adding a header that contains MAC addressing information and a trailer used for error checking. The header typically includes the source and destination MAC addresses, while the trailer contains a Frame Check Sequence (FCS) which is used for error detection¹.

The Data Link layer ensures that messages are delivered to the proper device on a LAN using hardware addresses and translates messages from the Network layer into bits for the Physical layer to transmit. It also controls how data is placed onto the medium and is received from the medium through the physical hardware.

References :=

- ? The OSI Model – The 7 Layers of Networking Explained in Plain English
- ? OSI Model - Network Direction
- ? Which layer adds both header and trailer to the data?
- ? What is OSI Model | 7 Layers Explained - GeeksforGeeks

NEW QUESTION 17

Which protocol allows you to securely upload files to another computer on the internet?

- A. SFTP
- B. ICMP
- C. NTP
- D. HTTP

Answer: A

Explanation:

SFTP, or Secure File Transfer Protocol, is a protocol that allows for secure file transfer capabilities between networked hosts. It is a secure extension of the File Transfer Protocol (FTP). SFTP encrypts both commands and data, preventing passwords and sensitive information from being transmitted openly over the network. It is typically used for secure file transfers over the internet and is built on the Secure Shell (SSH) protocol¹. References :=

- What Is SFTP? (Secure File Transfer Protocol)
- How to Use SFTP to Safely Transfer Files: A Step-by-Step Guide
- Secure File Transfers: Best Practices, Protocols And Tools

The Secure File Transfer Protocol (SFTP) is a secure version of the File Transfer Protocol (FTP) that uses SSH (Secure Shell) to encrypt all commands and data. This ensures that sensitive information, such as usernames, passwords, and files being transferred, are securely transmitted over the network.

- ICMP (Internet Control Message Protocol) is used for network diagnostics and is not designed for file transfer.
 - NTP (Network Time Protocol) is used to synchronize clocks between computer systems and is not related to file transfer.
 - HTTP (HyperText Transfer Protocol) is used for transmitting web pages over the internet and does not inherently provide secure file transfer capabilities.
- Thus, the correct protocol that allows secure uploading of files to another computer on the internet is SFTP.

References :=

- Cisco Learning Network
- SFTP Overview (Cisco)

NEW QUESTION 21

You need to connect a computer's network adapter to a switch using a 1000BASE-T cable. Which connector should you use?

- A. Coax
- B. RJ-11
- C. OS2 LC
- D. RJ-45

Answer: D

Explanation:

- 1000BASE-T Cable: This refers to Gigabit Ethernet over twisted-pair cables (Cat 5e or higher).
- Connector: RJ-45 connectors are used for Ethernet cables, including those used for 1000BASE-T.
- Coax: Used for cable TV and older Ethernet standards like 10BASE2.
- RJ-11: Used for telephone connections.
- OS2 LC: Used for fiber optic connections. References:
- Ethernet Standards and Cables: Ethernet Cable Guide

NEW QUESTION 26

A user reports that a company website is not available. The help desk technician issues a tracert command to determine if the server hosting the website is reachable over the network. The output of the command is shown as follows:

```
C:\>tracert 192.168.1.10
Tracing route to 192.168.1.10 over a maximum of 30 hops:
 0  ms  0  ms  1  ms  192.168.5.1
 1  ms  0  ms  0  ms  10.0.1.1
 2  *      *      *      Request timed out.
 3  ms  1  ms  0  ms  10.0.0.2
 4  ms  1  ms  0  ms  192.168.1.10
```

What can you tell from the command output?

- A. The router at hop 3 is not forwarding packets to the IP address 192.168.1.10.
- B. The server address 192.168.1.10 is being blocked by a firewall on the router at hop 3.
- C. The server with the address 192.168.1.10 is reachable over the network.
- D. Requests to the web server at 192.168.1.10 are being delayed and time out.

Answer: C

Explanation:

The tracert command output shows the path taken to reach the destination IP address, 192.168.1.10. The command output indicates:

- Hops 1 and 2 are successfully reached.
- Hop 3 times out, meaning the router at hop 3 did not respond to the tracert request. However, this does not necessarily indicate a problem with forwarding packets, as some routers may be configured to block or not respond to ICMP requests.
- Hops 4 and 5 are successfully reached, with hop 5 being the destination IP 192.168.1.10, indicating that the server is reachable.

Thus, the correct answer is C. The server with the address 192.168.1.10 is reachable over the network.

References :=

- Cisco Traceroute Command
- Understanding Traceroute

The tracert command output indicates that the server with the address 192.168.1.10 is reachable over the network. The asterisk (*) at hop 3 suggests that the probe sent to that hop did not return a response, which could be due to a variety of reasons such as a firewall blocking ICMP packets or the router at that hop being configured not to respond to ICMP requests. However, since the subsequent hops (4 and 5) are showing response times, it means that the packets are indeed getting through and the server is reachable12. References :=

- How to Use Traceroute Command to Read Its Results
- How to Use the Tracert Command in Windows

NEW QUESTION 29

Which standard contains the specifications for Wi-Fi networks?

- A. GSM
- B. LTE
- C. IEEE 802.11
- D. IEEE 802.3
- E. EIA/TIA 568A

Answer: C

Explanation:

The IEEE 802.11 standard contains the specifications for Wi-Fi networks. It is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 6 GHz1. This standard is maintained by the Institute of Electrical and Electronics Engineers (IEEE) and is commonly referred to as Wi-Fi. The standard has evolved over time to include several amendments that improve speed, range, and reliability of wireless networks.

References :=

- The Most Common Wi-Fi Standards and Types, Explained
- 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a
- Wi-Fi Standards Explained - GeeksforGeeks

=====

NEW QUESTION 31

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

100-150 Practice Exam Features:

- * 100-150 Questions and Answers Updated Frequently
- * 100-150 Practice Questions Verified by Expert Senior Certified Staff
- * 100-150 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 100-150 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 100-150 Practice Test Here](#)